

**The Specification**

Please replace the paragraph on page 1, lines 15-25, with the following paragraph:

Today, file storage is migrating toward a model in which files are stored on various networked computers, rather than on a central storage server. One challenge faced in storing files on remote computers concerns controlling access to files that may be distributed over many different computers in a manner that allows an authorized user to access a file while at the same time insuring that unauthorized users are prevented from accessing the file. A co-pending U.S. Patent Application Serial No. 09/814,259 entitled No. \_\_\_\_\_ entitled "On-Disk File Format for a Serverless Distributed File System", Attorney Docket No. MS1-733US, to inventors William J. Bolosky, Gerald Cermak, Atul Adya, and John R. Douceur describes a file format that provides such allowances and assurances. This application is hereby incorporated by reference.

Please replace the paragraph on page 10, line 19 – page 11, line 9, with the following paragraph:

For small files, the entire file is hashed and encrypted using convergent encryption, and the resulting hash value is used as the encryption key. The encrypted file can be verified without knowledge of the key or any need to decrypt the file first. For large files, the file contents are broken into smaller blocks and then convergent encryption is applied separately to each block. For example, the file  $F$  may be segmented into " $n$ " pages  $F^0$ - $F^{n-1}$ , where each page is a fixed size (e.g., a 4Kbyte size). Convergent encryption is then applied to the file at the block level. That is, each block  $F^i$  is separately hashed using a one-way hash function

(e.g., SHA, MD5, etc.) to produce a hash value  $h(F^i)$ . Each block  $F^i$  is then encrypted using a symmetric cipher (e.g., RC4, RC2, etc.) with the hash value  $h(F^i)$  as the key, or  $E_{h(F^i)}(F^i)$ , resulting in an array of encrypted blocks which form the contents of the file. For more information on block-by-block encryption, the reader is directed to co-pending U.S. Patent Application Serial No. 09/814,259 entitled No. \_\_\_\_\_ entitled "On-Disk File Format for a Serverless Distributed File System", Attorney Docket No. MS1-733US, to inventors William J. Bolosky, Gerald Cermak, Atul Adya, and John R. Douceur.